Curriculum Vitae
Silvio Micali

Ford Professor of Engineering
Electrical Engineering and Computer Science Department
Stata Center, Room G644, 32 Vassar Street, Cambridge, MA 02139
617 253 5949 silvio@csail.mit.edu

December 2018

Personal Data

Born in Palermo, Italy, October 13, 1954.
U.S. and Italian citizen

Education

- Laurea (*cum laude*) in Mathematics, University of Rome, March 1978
- Ph.D. in Computer Science, University of California—Berkeley, December 1983

Scientific Interests

- Cryptography
- Secure Protocols
- Pseudo-Random Number Generation
- Proof Systems
- Distributed Computation
- Zero Knowledge
- Mechanism Design
- Blockchains
- Cryptocurrencies

Selected Awards

- Turing Award (Computer Science)
- Gödel Prize (in Theoretical Computer Science)
- RSA Prize (in Cryptography)
- TCC Test-Of-Time Award (in Cryptography)
- Member, National Academy of Sciences
- Member, National Academy of Engineering
- Member, American Academy of Arts and Sciences
- Accademia Nazionale dei Lincei

- Frontier of Knowledge Award, BBVA Foundation
- Fellow, International Association of Cryptographic Research
- Palermitano nel Mondo
- Chair Professor, Tsinghua University
- Rademacher Lecturer, University of Pennsylvania
- Distinguished Alumnus Award, Computer Science and Engineering, UC Berkeley
- Laurea ad Honorem, University of Salerno
- Carnegie Corporation's "Great Immigrants: Pride of America"

Academic Appointments

Institution	*Position*	*Period*
MIT	Associate Head, EECS Dept.	2015-
MIT	Full Professor	1991-
MIT	Tenured Associate Professor	1988-1991
MIT	Associate Professor	1986-1988
MIT	Assistant Professor	1983-1986
University of Toronto	Post-doctoral Fellow	1982-1983

Doctoral Students

- Zeyuan Allen-Zhu, *Microsoft* (PhD, Summer 2015)
- Alessandro Chiesa, *UC Berkeley* (PhD September 2014)
- Pablo Azar, *PhD Student in Economics at MIT,* (EECS PhD September 2014)
- Jing Chen, *Stony Brook University* (PhD September 2012)
- Dr. Paul Valiant, *Brown University* (PhD June 2008)
- Prof. Rafael Pass, *Cornell University* (PhD. June 2006)
- Dr. Matt Lepinski, *BBN Technologies* (PhD. June 2006)
- Prof. Chris Peikert, *GeorgiaTech* (PhD. June 2006)
- Prof. Abhi Shelat , *NorthEastern University* (PhD. December 2005)
- Prof. Moses Liskov, *William and Mary* (PhD. June 2004)
- Prof. Leo Reyzin, *Boston University* (PhD. June 2001)
- Dr. Rosario Gennaro, *IBM,* (PhD. June 1996)
- Dr. Halevi, Shai, *IBM,* (PhD. June 1997)
- Dr. Ray Sidney *formerly, Google* (PhD. June 199)

- Prof. Rafail Ostrovsky, *University of California—Los Angeles* (PhD. June 1992)
- Prof. Mihir Bellare, *University of California—Sand Diego* (PhD.September 1991)
- Prof. Phil Rogaway, *University of California---Davis* (PhD. June 1991)
- Prof. Bonnie Berger, *Massachusetts Institute of Technology* (PhD. May 1990)
- Prof. Claude Crepeau, *University of Montreal* (PhD. February 1990)
- Dr. Pesech Feldman 1988

Post-Doctoral Fellows Hosted

- Dr. Alon Rosen
- Dr. Tal Rabin
- Dr. Oded Goldreich

Books

Randomness and Computation. S. Micali Editor,
5th volume of the series "Advances in Computing Research", JAI Press, December, 1989

Papers

JOURNALS

1. *Minimal forms in A-Calculus computations*
   Boehm C. and Micali S.
   Journal of Symbolic Logic, 45, March 1980, pp. 165-171

2. *Two way deterministic finite automata are exponentially more succinct than sweeping automata*
   Micali S.
   Information Processing Letters, 12 n. 2, April 13, 1981, pp. 103-105

3. *Probabilistic Encryption,*
   Goldwasser S. and Micali S.
   Journal of Computer and System Sciences, 28 n. 2, April 1984, pp 270-299

4. *How to generate Cryptographically Strong Sequences of Pseudo-Random Bits*
   Blum M. and Micali S.
   SlAM Journal on Computing, 13 no.4, November 1984, pp. 850-864

5. *Priority Queues with variable priority and an O(EV* log *V) Algorithm for finding a maximum weighted matching in general graphs*
   by Galil Z., Micali S. and Gabow H.
   SlAM Journal on Computing, 15 n. 1, February 1986, pp. 120-130

6. *How to Construct Random Functions*
   Goldreich 0., Goldwasser S. and Micali S.
   Journal of ACM, 33 n. 4, October 1986, pp. 792-807

7. *The Notion of Security for Probabilistic Cryptosystems*
   Micali S., Rackoff C. and Sloan B.

SlAM Journal on Computing, 17 n. 2, April 1988, pp. 412-426

8. *A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attack*
Goldwasser S., Micali S., and Rivest R.
SIAM Journal of Computing, 17 no 2, April 1988, pp. 281-308

9. *The Knowledge Complexity of Interactive Proof-Systems*
Goldwasser S., Micali S. and Rackoff C.
SlAM Journalon Computing, 18 n. 1, Feb. 1989, pp. 186-208

10. *A Fair Protocol for Signing Contracts*
Ben-Or M., Goldreich 0., Micali S. and Rivest R.
IEEE Trans. on Information Theory, 36 n. 1, January 1990. pp.40-46

11. *Proofs That Yield Nothing But their Validity, Or, All Languages in NP Have Zero-Knowledge Proofs*
Goldreich 0., Micali S. and Wigderson A.
Journal of ACM, 38 n. 3, July 1991, pp. 691-729

12. *Efficient, Perfect Polynomial Random Number Generators*
Micali S. and Schnorr C.
Journal of Cryptography, 3 n. 3, September 1991, pp.157-172

13. *Non-Interactive Zero-Knowledge*
Blum M., De Santis A., Micali S. and Persiano G.
SlAM J. on Computing, 20, December 1991, pp. 1084-1118

14. *How To Sign Given Any Trap-door Function*
Bellare M. and Micali S. Journal of ACM, 39, January 1992, pp. 214-233

15. *Mechanism for the T4 Lymphopenia of AIDS*
Micali S.
Proc. Natl. Acad. Sci. USA, Vol. 90, pp.10982-10983, December 1993

16. *On-Line/Off-Line Digital Signatures*
S. Even, 0. Goldreich and S. Micali.
Journal of Cryptography, 1996, 9, pp.35-67

17. *A secure Protocol for the Oblivious Transfer*
M. Fischer, S. Micali, and C. Rackoff.
Journal of Cryptography, 1996, pp. 1-5

18. *An Optimal Probabilistic Algorithm for Synchronous Byzantine Agreement*
P. Feldman and S. Micali.
SlAM Journal on Computing, August 1997

19. *Reducibility and Completeness In Multi-Party Private Computations*
J. Kilian, E. Kushilevitz, S. Micali, and R. Ostrovsky
SlAM J. on Computing, Vol. 29 Number 4 pp. 1189-1208, 2000

20. *Computationally Sound Proofs*
Silvio Micali
SICOMP Vol. 30, Number 4, pp.1253-1298, 2000

21. *Improving the Exact Security of Digital Signature Schemes*
S. Micali and L. Reyzin
Journal of Cryptography, 15, Winter 2002

22. *Optimal Error Correction for Computationally Bounded Noise*
S. Micali, C. Peikert, M. Sudan, and D. Wilson
IEEE Transactions on Information Theory, vol. 56, No. 11, November 2010, pp. 5673-5680

23. *Perfect Implementation*
S. Izmalkov, M. Lepinski, and S. Micali
Games and Economic Behavior, vol. 71, Issue 1, January 2011, pp. 121-140

24. *Collusive Dominant-Strategy Truthfulness*
J. Chen and S. Micali
Journal of Economic Theory, vol. 147, Issue 3, May 2012, Pages 1300-1312.

25. *The Order Independence of Iterated Dominance in Extensive Games*
J. Chen and S. Micali
Theoretical Economics (TE), Vol. 8, No. 1, January 2013, pp. 125-164

26. *Security Miracles, Secure Auctions, Matching Problem Verification*
S. Micali and M. Rabin
Transactions of the ACM, Vol. 57. No. 2, February 2014, pp. 85-93

27. *The Query Complexity of Scoring Rules*
P. Azar and S. Micali
Transactions on Economics and Computation (TEAC), Volume 2, Issue 3, Article 10, July 2014

28. *Sparse Johnson-Lindestrauss Matrices: Compression with Neurobiology-Based Constraints*
Z. Allen-Zhu, R. Gelashvili, S. Micali, and N. Shavit
Proceedings of the National Academy of Sciences (PNAS), November 2014

29. *Mechanism Design with Possibilistic Beliefs*
J. Chen and S. Micali
Journal of Economic Theory (JET), Vol. 156, pp. 77-102, March 2015.

30. *Tight Revenue Bounds with Possibilistic Beliefs and Level-k Rationality*
J. Chen, S. Micali, and R. Pass
Econometrica, Vol. 83, No. 4 (July, 2015), 1619–1639

31. *Knightian Analysis of the Vickrey Mechanism*
Z. Allen-Zhu, A. Chiesa, and S. Micali
Econometrica, Vol. 83, No. 5 (September, 2015), 1727–1754

32. *Physically Unclonable Values, Unforgeable Banknotes, and the Authentication of Arbitrary Objects*
S. Devadas and S. Micali
Communications of the ACM, to appear.

33. *Reconstructing Markov Processes from Independent Anonymous Experiments*
Z. Allen-Zhu and S. Micali
J. of Discrete Mathematics, Vol. 200, Issue C, pp 108-122, February 2016

34. *Leveraging Possibilistic Beliefs in Unrestricted Combinatorial Auctions*
J. Chen and S. Micali
Games, 2016, 7, 32; doi:10.3390/g7040032

35. *Collusion, Efficiency, and Dominant Strategies*
A. Deckelbaum and S. Micali
Games and Economic Behavior, 15 June 2017 (On Line)

36. *Computational Principal Agent Problems*
P. Azar and S. Micali
Theoretical Economics, on line. 2017.

REFEREED CONFERENCES AND WORKSHOPS

37. *Residually complete strategies and cofinal strategies*
Micali S.
Lambda Calcul et semantique formel des languages de programmation,
Actes de la 6Eme Ecole de Printemps d'Informatique Theorique, La Châtre 1978

38. *An* 0($E^{1/2}V$*) Algorithm for finding* a *maximum matching in general graphs*
Micali S. and Vazirani V.
21st Foundations of Computer Science (FOCS), Oct. 1980, pp 17-28

39. *Probabilistic Encryption and How to Play Mental Poker Keeping Secret All Partial Information*
Goldwasser S. and Micali S.
14th Symp. on Theory of Computing (STOC), San Francisco, CA, May 1982, pp.365-377

40. *Why and how to establish a private code*
Goldwasser S., Micali S. and Tong P.
23rd Foundations of Computer Science (FOCS), Chicago, Illinois, Nov. 1982, pp. 134-144

41. *Strong Signature Schemes*
Goldwasser S., Micali S. and Yao A.
15th Symp. on Theory of Computing (STOC), Boston, Massachusetts, May 1983, pp. 431-439

42. *How to simultaneously exchange a secret bit by flipping a symmetrically-biased coin*
Luby M., Micali S. and Rackoff C.
24th Foundations of Computer Science, November 1983, Arizona, pp.11-22

43. *On the cryptographic applications of poly-random function*
Goldreich 0., Golwasser S. and Micali S.
CRYPTO 84, Santa Barbara, California pp. 276-288

44. *Verifiable secret sharing and achieving simultaneity in the presence of faults*
Chor B., Goldwasser S., Micali S. and Awerbuch B.
Foundations of Computer Science (FOCS), Portland, Oregon, Oct. 1985, pp. 383-395

45. *Byzantine agreement in constant expected time (and trusting no one),* by
Feldman P. and Micali S.
Foundations of Computer Science (FOCS), Portland, Oregon, Oct, 1985, pp. 267-276

46. *Dynamic Deadlock Resolution Protocols*
Awerbuch B. and Micali S.
Foundations of Computer Science (FOCS), Toronto, Canada, Oct. 1986, pp. 196-207

47. *Proofs That Yield Nothing But Their Validity and a Methodology of Cryptographic Protocol Design*
Goldreich 0., Micali S. and Wigderson A.
Foundations of Computer Science (FOCS), Toronto, Canada, Oct. 1986, pp. 174-186

48. *How to Play any Mental Game or A completeness Theorem for Distributed Protocols with Honest Majority*
Goldreich 0., Micali S. and Wigderson A.
19th Symp. on Theory of Computing (STOC), New York, NY, May 1987, pp. 218-229

49. *Non-Interactive Zero-Knowledge And Its Applications*
Blum M., Feldman P. and Micali S.
20th Symp. on Theory of Computing (STOC), Chicago, Ill, May 1988, pp. 103-112

50. *Optimal Algorithms For Byzantine Agreement,*
Feldman P. and Micali S.
20th Symp. on Theory of Computing (STOC), Chicago, Ill, May 1988, pp. 32-42

51. *Everything provable is provable in zero knowledge*
Ben-Or M., Goldreich 0., Goldwasser S., Hastad J., Kilian J., Micali S. and Rogaway P.
CRYPTO 88, Santa Barbara, CA, August 1988, pp. 37-56

52. *Super efficient, perfect pseudo-random number generators*
Micali S. and Schnorr C.
CRYPTO 88, Santa Barbara, CA, August 1988, pp. 173-198

53. *An Improvement of the Fiat-Shamir Signature Identification and Signature Scheme*
Micali S. and Shamir A.
CRYPTO 88, Santa Barbara, CA, August 1988, pp. 244-247

54. *Non-Interactive zero-knowledge proof systems with auxiliary language*
De Santis A., Micali S. and Persiano G.
CRYPTO 88, Santa Barbara, CA, August 1988, pp. 269-282

55. *Perfect Pseudo-Random Generation*
Micali S.
IFIP 11th World Computer Congress, San Francisco, CA, August 1989. pp. 121-126

56. *Minimum Resource Zero-Knowledge Proofs*
Kilian J., Micali S. and Ostrovsky R.
30th Foundations of Comp. Sci. (FOCS), Research Triangle Park, North Carolina, Oct. 1989, pp. 474-479

57. *Perfect Zero Knowledge in Constant Rounds*
Bellare M., Micali S. and Ostrovsky R.
22nd Symp. on Theory of Computing (STOC), Baltimore, Maryland, May 1990, pp. 482-493

58. *The True Complexity of Statistical Zero Knowledge*
Bellare M., Micali S. and Ostrovsky R.
22nd Symp. on Theory of Computing (STOC), Baltimore, Maryland, May 1990, pp. 494-502

59. *The Round Complexity of Secure Protocols,* by
Beaver D., Micali S. and Rogaway P.
22nd Symp. on Theory of Computing (STOC), Baltimore, Maryland, May 1990, pp. 503-513

60. *Collective Coin Flipping Without Assumptions nor Broadcasting*
Micali S. and Rabin T.
CRYPTO 90, Lecture Notes in Computer Science, Vol. 537, Springer Verlag, 1990, pp. 253-266

61. *Secure Computation*
S. Micali and P. Rogaway
CRYPTO 91, Lecture Notes in Computer Science, Vol. 576, Springer Verlag, 1992, pp. 392-404

62. *Fair Public-Key Cryptosystems*
S. Micali
CRYPTO 92, Santa Barbara, CA, August 1992, pp. 3-11- 3-24

63. *New Approaches to Secret-Key Agreement*
T. Leighton and S. Micali
CRYPTO 93, Santa Barbara, CA, August 1993, pp. 38.1-38.11

64. *A Simple Method for Generating and Sharing Pseudo-Random Functions, with Applications to Clipper-Like Key Escrow Systems*
S. Micali and R. Sidney,
CRYPTO 95, Santa Barbara, CA, August 1995

65. *Practical and Provably-Secure Commitment Schemes from Collision-Free Hashing*
S. Halevi and S. Micali
CRYPTO 96, Santa Barbara, CA, August 1996

66. *Efficient Certificate Revocation*
S. Micali
RSA97, San Francisco, CA, January 1997

67. *Certified E-Mail with Invisible Post Offices*
S. Micali
RSA 97, San Francisco, CA, January 1997

68. *Computationally Sound Checkers For NP-complete Problems*
S. Micali
Mathematical Foundations of Computer Science 98, Prague, August 1998

69. *Computationally Private Information Retrieval*
C. Cachin, S. Micali, and M. Stadler
EUROCRYPT 99, Prague, Check Republic, May 1999

70. *Lower Bounds for Oblivious Transfer Reductions*
Y. Dodis and S. Micali
EUROCRYPT 99, Prague, Check Republic, May 1999

71. *The All-Or-Nothing Nature of Secure Computation*
Beimel A., T. Malkin and S. Micali
CRYPTO 99, Santa Barbara, CA, August 1999

72. *Verifiable Random Functions*
S. Micali, M. Rabin and S. Vadhan
40th Foundations of Computer Science (FOCS), New York, Oct 1999

73. *Public-key Encryption in a Multi-User Setting: Security Proofs and Improvements* by
M. Bellare, A. Boldyreva, and S. Micali
EUROCRYPT 2000, Bruges, Belgium, May 2000

74. *Resettable Zero Knowledge*
C. Canetti, 0. Goldreich, S. Goldwasser, and S. Micali
32nd Symposium On Theory of Computing (STOC), Portland, Oregon, May 2000

75. *Parallel Reducibility*
Y. Dodis and S. Micali
CRYPTO 2000, Santa Barbara, CA, August 2000

76. *Amortized E-Cash*
M. Liskov S. Micali

Financial Cryptography 2001, Anguilla, BWI, February 2001

77. *Min-Round Resettable Zero Knowledge*
S. Micali and L. Reyzin
EUROCRYPT 2001, May 2001

78. *Resettable Identification*
M. Bellare, M. Fischlin, S. Goldwasser, and S. Micali
EUROCRYPT 2001, May 2001

79. *Accountable-Subgroup Multisignatures*
S. Micali, K. Ohta, and L. Reyzin
8th ACM Conference on Computer and Communications Security, Philadelphia, Pennsylvania, November 2001

80. *Mutually Independent Commitment*
M. Liscov, A. Lysyanskaya, S. Micali, L. Reyzin and A. Smith
ASIACRYPT 2001

81. Fractal Merkle Tree Representation and Traversal
M. Jacobson, T. Leighton, S. Micali, and M. Szydlo
RSA 2003, San Francisco, CA, April 2003

82. *Micropayments Revisited*
S. Micali and R. Rivest
RSA 2002, San Jose, CA, 2002

83. Plaintext Awareness via Key Registration
J. Herzog, M. Liscov and S. Micali
CRYPTO 2003, Santa Barbara, CA, August 2003

84. *Simple and Fast Optimistic Protocols for Fair Electronic Exchange*
S. Micali
Principles of Distributed Computing Conference (PODC), 2003, Needham, MA 2003

85. NOVOMODO: Scalable Certificate Validation and Simplified PKI Management
S. Micali
Proceedings 1st Annual PKI Research Workshop, NISTIR 7059, October 2003

86. Zero-Knowledge Sets.
S. Micali, M. Rabin and J. Kilian
Foundations of Computer Science (FOCS), Cambridge, MA, October 2003

87. *Tamper Proof Security: Theoretical Foundations for Security Against Hardware Tampering*
R. Gennaro, A. Lysyanskaya, T. Malkin, S. Micali and T. Rabin
1st Theory of Cryptography Conference, Cambridge (TCC), Mass, February 2004

88. Physically Observable Cryptography
S. Micali and L. Reyzin
1st Theory of Cryptography Conference (TCC), Cambridge, Mass, February 2004

89. Sequential Aggregate Signatures from Trapdoor Permutations
A. Lyssyanskaya, S. Micali, L. Reyzin, and H. Shacham
EUROPRYPT 2004, Interlaken, Switzerland, May 2004

90. Completely Fair SFE and Coalition-Stable Cheap Talk
M. Lepinski, S. Micali, C. Peikert, and A. Shelat

PODC 2004, Canada, July 2004

91. Fair Zero Knowledge
M. Lepinski, S. Micali, and A. Shelat
Theory of Cryptography Conference (TCC), Cambridge, MA, February 2005

92. Optimal Error Correction Against Computationally Bounded Noise
S. Micali, C. Peikert, M. Sudan, and D. Wilson
Theory of Cryptography Conference (TCC), Cambridge, MA, February 2005

93. Collusion-Free Protocols
M. Lepinski, S. Micali, and A. Shelat
Symposium on Theory of Computing (STOC), Baltimore, ME, May 2005

94. Rational Secure Computation and Ideal Mechanism Design
S. Izmalkov, M. Lepinski and S. Micali
Foundation of Computer Science Conference (FOCS), Pittsburgh, PA, October 2005

95. Local Zero Knowledge
S. Micali and R. Pass
Symposium on Theory of Computing (STOC), Baltimore, ME, May 2006

96. Independent Zero-Knowledge Sets
R. Gennaro and S. Micali
33rd International Colloquium on Automata Languages and Programming (ICALP), Venice, Italy, July 2006

97. Input-Indistinguishable Computation
S. Micali, R. Pass, and A. Rosen
Foundation of Computer Science Conference (FOCS), Berkeley, CA, October 2006

98. Online-Untransferable Signatures
M. Liskov and S. Micali
PKC2008

99. Verifiably Secure Devices (and Correlated Equilibrium)
S. Izmalkov, M. Lepinski, and S. Micali
Theory of Cryptography Conference (TCC), New York, February 2008

100. Truly Rational Secret Sharing
S. Micali and abhi shelat
Theory of Cryptography Conference (TCC), San Francisco, March 2009

101. A New Approach to Auctions and Mechanism Design
J. Chen and S. Micali
Symposium on Theory of Computing (STOC), Washington, DC, May/June 2009

102. Guaranteeing Perfect Revenue From Perfectly Knowledgeable Players
J. Chen, A. Hassidim, and S. Micali
Innovations in Computer Science (ITCS), Beijing, China, January 2010

103. Leveraging Collusion in Combinatorial Auctions
J. Chen, S. Micali, and P. Valiant
Innovations in Computer Science (ITCS), Beijing, China, January 2010

104. Concrete And Perfect Implementation of Arbitrary Mechanisms
(A quick summary of joint work with Sergei Izmalkov and Matt Lepinski)

S. Micali
BQGT'10 May 14-16, 2010 Newport Beach, California USA

105. *Safe Rationalizability and Mechanism Design*
J. Chen and S. Micali
2nd Brazilian Workshop on Game Theory, July 29-August 4, 2010, Sao Paulo, Brazil

106. *Crowdsourced Bayesian Auctions*
P. Azar, J. Chen, and S. Micali
Innovations in Theoretical Computer Science (ITCS), Jan 2012
(Also: North American Summer Meeting of the Econometric Society, St. Luis, June 2011)

107. *Knightian Auctions*
A. Chiesa, S. Micali, and Z. Zhu
Innovations in Theoretical Computer Science (ITCS), Jan 2012

108. *Rational Proofs*
P. Azar and S. Micali
Symposium on Theory of Computing (STOC), May 2012

109. *Parametric Digital Auctions*
P. Azar and S. Micali
Innovations in Theoretical Computer Science (ITCS), Jan 2013

110. *Optimal and Efficient Parametric Auctions*
P. Azar, C. Daskalakis, M. Weinberg, and S. Micali
Symposium on Discrete Algorithms (SODA) Jan 2013

111. *Knightian Self-Uncertainty in the VCG Mechanism in Unrestricted Combinatorial Auctions*
A. Chiesa, S. Micali, and Z. Zhu
Economics and Computation (EC), 2014

112. *Better Outcomes from More Rationality*
J. Chen, S. Micali, and R. Pass
Innovations in Theoretical Computer Science (ITCS), Jan 2015

113. *Single-Good Auctions with Externalities*
J. Chen and S. Micali
2015 Econometric Society World Congress

114. *Mechanisms with Costly Knowledge*
A. M. Ileri and S. Micali
2016 Innovations in Theoretical Computer Science

115. *Auction Revenue in the General Spiteful-Utility Model*
J. Chen and S. Micali
2016 Innovations in Theoretical Computer Science

116. *Fast and Furious Byzantine Agreement*
S. Micali
2017 Innovations in Theoretical Computer Science

117. *Scaling Byzantine Agreement for Cryptocurrencies*
Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich
2017 Symposiumon Operating Systems Principles (SOSP)

Lectures

"Residually complete strategies and cofinal strategies"

1. École d'Informatique Theorique, La Chatre, 1978

"Two-way automata versus sweeping automata "

2. University of Rome, July 1980

"An $0\{V^{1/2}E)$ *algorithm for maximum matching in general graphs"*

3. Foundations of Computer Science Conference, Syracuse, October 1980.
4. University of California -Berkeley, November 1980
5. University of Toronto, Spring 1982

"Coin Flipping by telephone"

6. Massachusetts Institute of Technology, LOS, December 1981
7. University of California -Berkeley, December 1981
8. Stanford University, Spring 1982
9. Brown University, Spring 1982
10. Pennsylvania State University, Spring 1982
11. University of Toronto, Spring 1982
12. IBM Research - Yorktown Heights, Spring 1982
13. Bell Laboratories, Spring 1982
14. Cornell University, Spring 1982
15. Columbia University, Spring 1982
16. New York University, Spring 1982
17. Xerox Park, Spring 1982
18. University of Southern California, Spring 1982
19. University of Rome, July 1982

"How to generate cryptographically strong sequences of pseudo-random bits "

20. American Mathematical Society Conference on Probabilistic Methods, June 1982

21. Foundations of Computer Science Conference, Chicago, November 1982
22. 1983 Theory Day, Columbia University, Spring 1983
23. Yale University, Spring 1983
24. Carnegie Mellon University, Spring 1983
25. University of Waterloo, Spring 1983
26. Massachusetts Institute of Technology -Applied Mathematics, Spring 1983
27. University of New York at Buffalo, Spring 1983
28. University of Pisa, July 1983
29. Mathematisch centrum, Amsterdam, November 85

"Probabilistic Encryption"

30. University of Toronto, Fall 1982

"Probabilistic Digital Signatures"

31. Harvard University, Spring 1983
32. Symposium on Theory of Computing, Boston, MA, Spring 1983

"How to simultaneously exchange a secret bit"

33. University of California -Berkeley, June 1983
34. Yale University, June 1983
35. University of Toronto, June 1983
36. University of Zurich, July 1983
37. Massachusetts Institute of Technology, Fall 1983
38. University of Chicago, March 1984

"A provably correct oblivious transfer"

39. Eurocrypt ‘84, Paris, April 1984

"How to construct Random Functions"

40. University of Toronto, December 1983
41. Days of Study of Algorithms (Opening lecture), Rome, January 1984

42. University of Pittsburgh, February 1984
43. University of California -Berkeley, March 1984
44. IBM Research -San Jose, March 1984
45. University of Chicago, March 1984
46. Rensselaer Polytechnic Institute, Spring 1984
47. Foundations of Computer Science Conference, Florida, October 1984
48. Mathematisch centrum, Amsterdam, November 1985

"Interactive proof systems"

49. University of Chicago, March 1984
50. University of California -Berkeley, March 1984
51. Massachusetts Institute of Technology, May 1984
52. Boston College, Boston, MA, February 1986

"Knowledge Complexity"

53. American Mathematical Society Meeting, Complexity Theory Day, August 1984
54. Massachusetts Institute of Technology, LCS, December 1984
55. University of Southern California, January 1985
56. University of California-Berkeley, January 1985
57. University of Toronto, February 1985
58. Cornell University, February 1985
59. Symposium on Theory of Computing, Providence, RI, May 1985
60. Brown University, Providence, RI, September 1985
61. Boston University, Boston, MA, October 1985

"How to transform a semi-synchronous network to a simultaneous one"

62. Harvard University, December 1984
63. IBM-San Jose, January 1985

"A protocol for signing contracts fairly"

64. Colloquium on Automata, Languages and Programming, Nafplio, Greece, July 1985

"A Methodology for Proving the Correctness of Cryptographic Protocols"

65. Brown University, Providence, Ill, October 1985

66. Mathematisch Centrum, Amsterdam, The Netherlands, November 1985

"A new Look at Algorithmic Randomness"

67. Dartmouth University, Hanover, NH, January 1986

"Knowledge and Efficient Computation"

68. First Conference on Theoretical Aspects of Reasoning About Knowledge, Asilomar, CA, March 1986

"Proofs That Release Minimum Knowledge

69. Conference on Randomness and Computation, Marseille, France, March 1986

"All of NP possess Zero-Knowledge Proofs"

70. Workshop on Probabilistic Computation, Luminy, France, March 1986

71. University of Toronto, Toronto, Canada, April 1986

"All You Always Wanted From a Cryptographic Protocol and Never Dared to Ask"

72. LCS, MIT, Cambridge, MA, May 1986

"How to Compile Protocols for Reliable Players to Equivalent Fault-Tolerant Protocols"

73. Mathematical Sciences Research Institute, Berkeley, CA, May 1986

74. Yale University, April 1986

"Recent Trends in Complexity Based Cryptography"

75. Centro Ricerche per le Applicazioni Industriali, July 1986

"Proofs, Knowledge and Computation"

76. Mathematical Foundations of Computer Science Conference, Bratislava, Czechoslovakia, August 1986

77. York University, Toronto, Canada, October 1986

78. Meeting on Complexity Theory, Oberwolfach, Germany, November 1986

79. Carnegie-Mellon University, Pittsburgh, PENN, December 1986

80. IEEE Information Theory Workshop, Bellagio, Italy, June 1987

81. Interdisciplinary Conference on Randomness, Columbus, Ohio, April 1988

82. University of Illinois at Urbana Champaign, Urbana, Illinois, October 1988

83. Mathematics Colloquium, Princeton University, Princeton, New Jersey, October 1988

"Detecting and Resolving Dynamic Deadlocks"

84. Foundation of Computer Science Conference, Toronto, Canada, October 86

"The Completeness Theorem for Protocols with Honest Majority"

85. University of Salerno, Salerno, Italy, July 86

86. Yale University, New Haven, CONN, December 86

87. University Of Rome, Rome, Italy, January 87

88. University Of Toronto, Toronto, Canada, March 87

89. 19th ACM Symp. on Theory of Computing, New York, NY, May 87

90. University of Zurich, Zurich, Switzerland, July 87

"Interactive Proofs, Zero Knowledge, and Applications"

91. Center for intelligent control Systems, MIT, May 1988

"Byzantine Agreement in constant expected time"

92. Yale University, New Haven, CONN, July 1987

"Nothing But The Truth"

93. 25th Anniversary of the Laboratory for Computer Science, MIT, November 1988

"An optimal Algorithm for Byzantine Agreement from Scratch II

94. Meeting on Complexity Theory, Oberwolfach, Germany, November 1988

95. Workshop on Randomness and Computation, MIT, November 1988

96. Technion, Haifa, Israel, January 1989

97. 16th International Colloquium on Automata, Languages and Programming, Stresa, Italy, July 1989

98. Carnegie Mellon University, Pittsburg, Penn., October 1989

"Non-Interactive Zero-Knowledge and Security Against Chosen Cyphertext Attack"

99. CRYPTO 88, Santa Barbara, California, August 1988

"Efficient, Perfect Pseudo-Random Generation"

100. CRYPTO 88, Santa Barbara, California, August 1988

"Digital Signatures: From Theory to Practice

101. National Security Agency Course of Instruction, MD, February 1989

"Perfect Zero-knowledge, Constant- Round Proof for Graph Isomorphism "

102. University of California, Berkeley, CA, May 1989

103. University of Toronto, Toronto, Canada, June 1989

"How to collectively flip a coin"

104. Scuola Normale Superiore, Pisa, Italy, July 1989

105. CRYPTO 89, Santa Barbara, CA1 August 1989

"On-line/Off-line Digital Signatures"

106. Crypto 89, Santa Barbara, CA, August 1989

"Digital Signatures: The Evolution of A Fundamental Primitive"

107. CRYPTO 89, Santa Barbara, CA, August 1989

"Perfect Pseudo-Random Number Generation"

108. 11th World Computer Congress, San Francisco, CA, August 1989

"Proving Properties of Physically Hidden Data"

109. International Computer Science Institute, Berkeley, CA, August 1989

110. International Workshop on Cryptography, Oberwolfach, Germany, September 1989

"Card Games Are Universal"

111. University of Rome, Rome, Italy, January 1990

112. University of Toronto, Toronto, Ontario, Canada, January 1990

"Probabilistic Proofs and Their Applications"

113. American Association for the Advancement of Science Meeting, New Orleans, LA, February 1990

"Zero-Knowledge Proofs and Their Applications"

114. Harvard University, Cambridge, MA, April 1990

115. Yale University, New Haven, CT, April 1990

"The Round Complexity of Secure Protocols"

116. Princeton University, Princeton, NJ, May 1990

117. Theory Day, University of Maryland, MD, November 1990

"Verifiable Secret Sharing"

118. Laboratory for Computer Science, MIT, May 1990

"Cryptographic Security"

119. Center for Advanced Engineering, Study, MIT, May 1990

"Secure Computation"

120. MIT's Lab for Computer Science Summer Meeting, Chatham, Mass, June 1990

"The Security of Digital Signature Schemes"

121. Algorithms and Complexity, 2nd International School for Computer Science Researchers, Acireale, Italy, June, 1990

"The Security of Public Key Cryptosystems"

122. Algorithms and Complexity, 2nd International School for Computer Science Researchers, Acireale, Italy, June, 1990

"A Pseudo-Random Generator Based on the Discrete Logarithm"

123. Algorithms and Complexity, Second International School for Computer Science Researchers, Acireale, Italy, June, 1990

"Simple and Efficient Primality Testing"

124. Algorithms and Complexity, Second International School for Computer Science Researchers, Acireale, Italy, June, 1990

"Digital Security for Bank Transactions"

125. Banca d'Italia, Rome, Italy, July, 1990

"Collective Coin Flipping Without Assumptions nor Broadcasting"

126. Crypto 90, Santa Barbara, California, August 1990

"Perfect Verifiable Secret Sharing Without Broadcasting"

127. Crypto 90, Santa Barbara, California, August 1990

"The Notion of Secure Computation"

128. DIMACS Workshop on Cryptography, Princeton University, Princeton, New Jersey, October 1990

"Secure Personal Identification"

129. Texas Instruments, TX, November 1990

130. EECS Colloquium, MIT, April 1991

"Zero-Knowledge Proofs"

131. Italian Mathematical Society, Bologna, Italy, May 1991

"*The Notion of Secure Computation"*

132. Crypto '91 Conference, Santa Barbara, CA, August 1991

"Probabilistic Potential: A Theory of T- Cell Differentiation"

133. Institut Pasteur, Paris, France, January 1992

"A Mechanism for AIDS' T4-Cell Loss"

134. International Computer Science Institute, Berkeley, CA, August 1992

135. Laboratory for Computer Science, MIT, Cambridge MA, November 1992

136. Cornell University, April 1993

137. 25th Annual ACM Symposium on the Theory of Computing (Special, out-of-program Lec- ture), San Diego, CA, May 1993

138. 37th Joint National Meeting of The Institute for Management Sciences/Operation Research Society of America, Boston, MA: April 1994

"Fair Public-Key Cryptosystems"

139. Crypto '92 Conference, Santa Barbara, CA, August 1992

140. 1992 Conference on Complexity Theory, Oberwolfach, Germany, November 1992

141. National Institute for Standard and Technology, Gaithersburg, MD, November, 1992

142. MIT-U.S. Government Workshop on Fair Cryptosystems, MIT, Cambridge, MA, April 1993

143. University of California, Berkeley, May 1993

144. The International Symposium on Technology and Society, Washington, DC, October 1993

"Advances in Cryptography"

145. 12th World Computer Congress, Madrid, Spain, September 1992

"Computation has Short Certificates"

146. Cornell University, Ithaca, NY, April1993

147. University of Toronto, Toronto, Canada, April 1993

148. State University of New York, Buffalo, NY, May 1993

149. University of California, Berkeley, CA, May 1993

150. Laboratory for Computer Science, MIT, June 1993

151. Harvard University, Cambridge, MA, October 1993

"New Approaches to Secret-Key Exchange"

152. Crypto 93 Conference, Santa Barbara, CA, August 1993

"Fair Cryptosystems and the Clipper Chip"

153. National Institute of Standards and Technology, Gaithersburg, MD, November 1993

154. The Boston Chapter of the ACM, Cambridge, MA, November 1993

"CS Proofs"

155. University of Rome, Rome, Italy, December 1993

156. Weizmann Institute of Sciences, Rehovot, Israel, January 1994

157. Yale University, New Haven, Connecticut, February 1994

"Which Key Escrow, If Any?"

158. MIT, Laboratory for Computer Science, April 1994

159. Eurocrypt 94, Perugia, Italy, May 1994

160. National Institute of Standards and Technology, Gaithersburg, MD, June 94

"CS Proofs and Computational Correctness"

161. University of Rome, Rome, Italy, July 94

162. International Combinatorics Conference in Honor of Adriano Garsia, Taormina, Italy, July 1994

163. University of California, Berkeley, CA, August 94

164. University of Toronto, Toronto, Canada, October 94

165. Applied Mathematics Colloquium, MIT, November 94

166. 1994 Conference on Complexity Theory, Oberwolfach, Germany, November 1994

167. 35th Foundation of Computer Science Conference, Santa Fe, New Mexico, November 1995

168. Johan Wolfgang Goethe University, June 1995

169. International Logic Symposium, Haifa, Israel, August 1995

"Unstealable Electronic Passwords"

170. Yale University, New Haven, May 1995

171. Johan Wolfgang Goethe University, June 1995

"CS Checking"

172. Cornell University, Ithaca, New York, May 1995

173. Technion, Haifa, Israel, June 1995

"Interactive and Zero-Knowledge Proofs"

174. International Logic Symposium, Haifa, Israel, August 1995.

"Compact Certification of Public Keys"

175. PKI Workshop, MITRE Corp., McLean, Virginia, September 1995

"An Efficient and Secure Digital Signature Scheme"

176. National Institute of Standards and Technology, Gaithersburg, MD, January 1994

177. MIT, Cambridge, Mass, December 1995

"Provably Secure Commitment Schemes from Collision-Free Hashing"

178. Brown University, Providence, RI, Apri11996

"Enhanced Certificate Revocation"

179. Federal PKI Meeting, Washington, DC, November 1995

180. Internet Privacy and Security Workshop, Haystack Observatory, Groton, MA, May 1996

181. ANSI Meeting, Cryptologic History Museum, Baltimore- Washington, September 96

182. RSA97 Conference, San Francisco, CA, January 1997

183. LIPARI 2000, Lipari, Italy, July 2000

"Certified E-Mail with Invisible Post Offices"

184. RSA97 Conference, San Francisco, CA, January 1997

"Complexity Preserving Checkers"

185. M. Rabin's Symposium, Jerusalem, Israel, June 1997

"Simultaneous Electronic Transactions with "Hand-Off" Trusted Parties"

186. Laboratory for Computer Science, MIT, March 1998

"Computationally-Sound Checkers for NP-Complete Problems"

187. Laboratory for Computer Science, MIT, April 1998

188. International Conference in Theoretical Computer Science in Honor of M. Blum, Hong Kong, April 1998

189. Workshop on Interactive Proofs:, PCP, and Fundamentals of Cryptography, Toronto, May 1998

190. Mathematical Foundations of Computer Science 98, Prague, August 1998

191. Laboratory for Information Decision Systems, MIT, October 1998

"A Stronger Definition of Proofs of Knowledge"

192. Workshop On Multi-Party Secure Computation, Weizmann Institute, Israel, June 1998

"The Notion of Secure Function Evaluation"

193. Workshop On Multi-Party Secure Computation, Weizmann Institute, Israel, June 1998

"Secure Protocols With Invisible trusted Parties"

194. Workshop On Multi-Party Secure Computation, Weizmann Institute, Israel, June 1998

195. Brandeis University, Waltham, MA, September 1998

196. Moses' Seminar, MIT, September 1998

197. Boston University, Boston, October 1998

198. Telecordia Laboratories, New Jersey, August 1999

"Computationally Private Information Retrieval with Polylogarithmic Communication"

199. Laboratory For Computer Science, MIT, October 1998

"Verifiable Random Functions"

200. Laboratory for Computer Science, MIT April 1999

"The All-Or-Nothing Nature of Secure Computation"

201. University of Toronto, Toronto, Canada, May 1999

202. University of California, Berkeley, CA, August 1999

203. Carnegie Mellon University, Pittsburgh, PA, February 2000

"Efficient ID and Signature Scheme based on Factoring"

204. PKI Standard Committee, Santa. Barbara, CA, August 1999

"Certified E-Mail with Invisible Post Offices"

205. Carnegie Mellon University, Pittsburgh, PA, February 2000

206. Industrial Liaison Program, FIB'V Workshop, MIT, May 2000

"Resettable Zero Knowledge"

207. The Fields Institute of Mathematical Sciences, Toronto, Canada, April 2000

208. 32nd Ann. Symposium On Theory of Computing, Portland, Oregon, May 2000

"Cryptographic Algorithms in The real World"

209. Carnegie Mellon University, Pittsburgh, Pennsylvania, May 2000

"Fair Protocols with Invisible Trusted Parties"

210. IdeaStream Conference, MIT, Cambridge, Mass, February 28, 2001

"Min Round Resettable Zero Knowledge"

211. Eurocrypt 2001, lnnsbruck, Austria, May 2001

"Zero Knowledge has come of age"

212. Invited Lecture, Eurocrypt 2001, Innsbruck, Austria, May 2001

"Fair Electronic Exchange"

213. Distinguished Lecture, Princeton University, October 2001

214. Invited Lecture, PODC 2003 Conference, Needham, Mass, August 2003

215. SUN Computers, Burlington, Mass, July 2003

216. Distinguished Lecture, Georgia Tech, Atlanta, GA, October 2003

217. Technion, Haifa, Israel, November 2003

218. University of California - Los Angeles, February 2004

219. RSA 2004 Conference, San Francisco, CA, February 2004

220. Venture One Exchange, Boston, MA, October 2004

221. City University of Hong Kong, Hong Kong, China, December 2004

222. University of Pennsylvania, PA, October 2005

223. University of California, Davis, May 2007

224. Boston University, May 2007

225. CIPS 2008, MIT, May 2008

"Zero-Knowledge Sets"

226. MIT's Laboratory for Computer Science, Cambridge, Mass, October 2003

227. University of Toronto, Toronto, Ontario, Canada, October 2003

228. Boston University, Boston, Mass, November 2003

229. Technion, Haifa, Israel, November 2003

230. Princeton's University, Princeton, NJ, December 2003

231. New York University, March 2004

232. IBM, Armonk, NY, March 2004

"Peppercoin Micropayments"

233. MIT's Technology Breakfast Series, MIT, December 2003

234. City University of Hong Kong, Hong Kong, China, December 2004

"Physically observable Cryptography"

235. Laboratory for Computer Science, MIT, Fall 2003

236. SUN Microsystems, Burlington, MA, January 2004

237. Theory of Cryptography Conference, February 2004

"Collusion-Free Protocols"

238. DIMACS Workshop on Formal Protocols, Rutgers U., NJ, June 2004

239. Princeton University, Princeton, NJ, June 2004

240. University of Toronto, Toronto, Canada, September 2004

241. Carnegie-Mellon University, Pittsburgh, September 2004

242. University of California, Berkeley, CA, November 2004

243. Theory Day, Courant Institute, New York University, NY, November 2004

244. Brown University, Providence, RI, April 2005

245. Cornell University, Ithaca, NY, April 2005

246. University of Pennsylvania, PA, October 2005

"How To Reach Correlated Equilibrium"

247. University of California, San Diego, CA, November 2004

248. Stanford University, Palo Alto, CA, November 2004

249. Computer Science and Artificial Intelligence Laboratory, MIT, December 2004

"Rational Secure Computation and Ideal Mechanism Design"

250. Computer Science and Artificial Intelligence Laboratory, MIT, May 2005

251. Hebrew University, Jerusalem, Israel, May 2005

252. University of Haifa, Haifa, Israel, May 2005

253. Conference on Computation and Game Theory, Stony brook, NY, July 2005

254. University of California, Berkeley, CA, September 2005

255. Stanford University, Palo Alto, CA, September 2005

256. University of Pennsylvania, PA, October 2005

257. Boston University, MA, November 2005

258. Institute for Advanced Studies, Princeton, NJ, November 2005

259. Columbia University, New York, NY, November 2005

260. University of Chicago, March 2006

261. Carnegie Mellon University, April 2006

262. Brown University, October 2006

"Transparent Computing and Correlated Equilibrium"

263. Microsoft Research, Redmond, Washington, October 2006

264. New York University, November 2006

265. Institute for Advanced Studies, Princeton, NJ, November 2006

266. Weizmann Institute of Science, Rehovot, Israel, January 2007

267. Hebrew University, Jerusalem, Israel, January 2007

268. North Eastern University, Boston, January 2007

"From Weakness to Strength"

269. Workshop on Creativity, MIT, November 2006

"Collusion-Resilient Revenue in Combinatorial Auctions"

270. Ehud Kalai Conference, Hebrew University, Israel, December 2007

"Verifiably Secure Devices"

271. Theory of Cryptography Conference, NYU, New York, February 2008

"Cryptographic Game Theory"

272. Special Panel Presentation, TCC 2008, NYU, New York, February 2008

"Resilient Mechanism Design"

273. Frontiers in Game Theory and Networked Controlled Systems, MIT, October 2008

274. First China Symposium in Theoretical Computer Science, Beijing, October 2008

275. University of Toronto, Ontario, Canada, October 2008

276. University of Tel Aviv, November 2008

277. Hebrew University, Jerusalem, November 2008

278. Microsoft New England, Cambridge, December 2008

279. Google, New York, January 2009

280. Institute for Advanced Studies, Princeton, January 2009

"Truly Rational Secret Sharing"

281. Theory of Cryptography Conference, San Francisco, California, March 2009

"A New Approach to Auctions and Mechanism Design"

282. Cornell University, Ithaca, NY, January 2009

283. University of Illinois, Urbana Champaign, March 2009

284. Northwestern University, Chicago, March 2009

285. Computer Science Department, UC Berkeley, Berkeley, California, March 2009

286. Science and Artificial Intelligence Laboratory, MIT, May 2009

287. Microsoft Research, Mountain View, California, June 2009

288. North American Summer Meeting of the Econometric Society, Boston University, June 2009

289. Department of Economics, Boston University, Boston, September 2009

290. Department of Economics, MIT, Cambridge, Mass, September 2009

291. China 2020 Vision Conference, Tsinghua University, Beijing, China, October 2009

292. School of Information and Communication, École Polytechnique Federal de Lausanne, April 2010

"Theory, Practice, and Fair Electronic Exchange"

293. Drexler University, Philadelphia, April 2010

"Perfect Revenue From Perfectly Informed Players"

294. Stanford University, Economics Department, May 2010

295. Weizman Institute, Rehovot, Israel, June 2010

"Perfect Implementation of Arbitrary Mechanisms"

296. Behavioral and Quantitative Game Theory, May 2010 Newport Beach, California USA

297. Decentralized Mechanism Design, Distributed Computing, and Cryptography Workshop, Princeton 2010

"Conservative Rationalizability"

298. Workshop On Solution Concepts For Extensive Games, Aarhus, Denmark, June 2010

"The Conservative Model of Incomplete Information and The Second-Knowledge Mechanism"

299. 2nd Brazilian Workshop on Game Theory, July 2010, Sao Paulo, Brazil

"25 Years of Zero Knowledge"

300. CRYPTO 2010, Santa Barbara, California, August 2010

"New Mechanisms For a New World"

301. University of Pennsylvania, Philadelphia, Pennsylvania, September 2010

"Resilient and Budget-Balanced Maximization of Social Welfare in Complete-Information Markets"

302. Tsinghua University, Beijing, China, January 2011

"Collusive Dominant-Strategy Truthfulness"

303. Innovation in Algorithmic Game Theory, Jerusalem, Israel, May 2011

"The Second-Knowledge Mechanism"

304. Cornell University, Ithaca, New York, September 2010

305. Microsoft New England, October 2010

306. Stanford University, November 2010

307. Tsinghua University, Beijing, China, January 2011

308. MIT, Theory of Computation Colloquium, February 2011

309. Columbia/NYU/IBM Theory Day, New York, NY, May 2011

310. Center for Rationality, Jerusalem, Israel, May 2011

311. Carnegie Mellon University, November 2011

"Virtually Trusted Electronic Communications and Transactions"

312. Citi-MIT Meeting, New York, June 2012

"Resilient Combinatorial Auctions"

313. Finance Made Difficult, MIT, June 2012

"Knightian Auctions"

314. Theory of Computation Colloqium, MIT, February 2012

315. Cornell University, March 2012

316. SIAM Conference, Halifax, Canada, June 2012

317. Theoretical Computer Science Workshop, City University, Hong Kong, July 2012

318. Harvard University, October 2012

319. New Economic School, Moscow, November 2012

320. Carnegie Mellon University, November 2012

"*Perfect Pseudo Randomness"*

321. Turing 100, Boston University, November 2012

"Universal Payment Systems"

322. Yandex, Moscow, November 2012

"Rational Proofs"

323. Newton Institute, Cambridge, England, April 2012

324. MIT, May 2012

325. Cambridge Area Economics and Computer Science Conference, Cambridge, MA April 2013

326. Hidelberg Laureate Forum, Hidelberg, Germany, September 2013.

327. Pneueli Lecture, Weizman Institute, Rehovot, Israel, December 2013

328. University of Venice, Venice, Italy, December 2013

"Fair Electronic Exchange"

329. MIT, World Federation of Exchnages Forum, December, 2013

"Proofs, Secrets, and Computation"

330. Lectio Magistralis, La Sapienza University, Rome, Italy, May 2013

331. University of Washington, Seattle, Distinguished Lecture, November 2013

332. WPI, Worcester, Distinguished Lecture, November 2013

333. MIT, CSAIL, Dertouzos Lecture, December 2013

334. Weizman Institute, Rehovot, Israel

335. Lectio Magistralis, Politecnico di Milano, Milan, Italy, December 2013

336. Lectio Magistralis, Universita' di Venezia, Venice, Italy, December 2013

337. Lectio Magistralis, Universita' di Palermo, Palermo, Italy, December 2013

338. Stony Brook University, University Distinguished Lectures in Science and Engineering, February 2014

339. Florida International University, Distinguished Lecture, October 2014

340. Russian-American Research Symposium, Moscow, Russia, December 2014

341. Global Lecture, Zhejiang University, Hangzhou, China, December 2014

342. Keynote Lecture, Techfest 2015, Indian Institute of Technology, Mumbay, India, Jan 2015

343. Infosys, Bangalore, India, Jan 2015

344. Lectio Magistralis, University of Salerno, Salerno, Italy, May 2015

345. Lectio Magistralis, University of Padova, Padova, Italy, May 2015

346. Distinguished Lecture, Pierre and Marie Curie University, Paris, France, May 2015

347. Science and Innovation Forum, Fudan University, Shanghai, Dec 2015

"Towards Resilient Mechanism Design"

348. Intel, November 2013

349. Theory of Cryptography Conference, Invited Lecture, San Diego, CA, February 2014

350. Distinguished Lecture, Indian Institute of Science, Bangalore, India, Jan 2015

351. French Symposium on Games 2015, Diderot University, Paris, France, May 2015

"Proofs (according to Silvio)"

352. Turing Lecture, STOC, New York, June 2014

"Knightian Analysis of the VCG Mechanism"

353. Invited Lecture, Games and Decision, Pisa, Italy, July 2014

"Rational Resilient Protocols"

354. Invited Lecture, PODC, Paris, July 2014

"The Mathematics of Secure Interaction"

355. Distinguished Lecture, Beijing University, Beijing, China, May 2015

"New Electronic Infrastructures"

356. Zhongzhi Enterprise Group, Beijing, China, May 2015

"Universal Micro Payments"

357. Zhongzhi Enterprise Group, Beijing, China, May 2015

"Prove, Segreti e Computazione"

358. Lectio Magistralis, Università di Genova, November 2016

"Evoluzione del Concetto di Prova"

359. Festival Della Scienza, Genova, November 2016

"Byzantine Agreement, Made Trivial"

360. Innovations in Theoretical Computer Science, UC Berkeley, January 2017

"Byzantine Agreement on Steroids"

361. Randomness, Complexity, and Cryptography, Weizman, Israel, April 2017

"Algorand"

362. IDSS Workshop on Data Analytics and Risk, MIT, April 2016

363. A Celebration of Mathematics and Computer Science, Institute of Advanced Studies, Princeton, October 2016

364. Symposium on Interdisciplinary Information Sciences, Tsinghua University, Beijing, December 2016

365. Theory of Computation Colloquium, CSAIL, MIT, February 2017

366. Boston University, Boston, Massachuesetts, March 2017

367. Keynote Lecture, Financial Cryptography Conference, Malta, April 2017

368. A New Generation of Blockchains, Italian Embassy, Wshington, DC, April 2017

369. Fintech Roundtable, Washington, DC, May 2017

370. CSAIL and MIT Alumni Connection, New York, NY, May 2017

371. CSAIL Allience Meeting, MIT, June 2017

372. Distinguished Lecture, University of Waterloo, Canada, June 2017

373. Keynote Lecture, WiSec 2017, Boston, July 2017

374. Media Lab, MIT, July 2017

375. Invited Lecture, Ai Decentralized, Toronto, Canada, July 2017

376. Keynote Lecture, First Pan-European ACM Conference, Barcelona, Spain, September 2017.

377. Cornell Tech, New York, NY, September 2017.

378. CESC, Berkeley, CA, October 2017

379. ACM Webinar, October 2017

380. Cambridge Blockchain Meetup, Cambridge, MA, November 2017

381. ECB Conference on Digital Transformation of the Retail Payments Ecosystem, Rome, December 2017

382. Ant Financial, Hanzhou, China, December 2017

383. World Internet Conference, Wuzhen, China, December 2017

"Computazione, Segreti e Casualità"

384. Accademia dei Lincei, Roma, November 2017

385. Accademia delle Scienze, Roma, November 2017

"Global Digital Economy and Technology"

386. Closing Remarks, World Internet Conference, Wuzhen, China, December 2017

"ALGORAND: The Truly Distributed Ledger"

387. Ant Technology Exploration Conference, Silicon Valley, January 2018

388. The FIELS Institute, Toronto, Canada, February 2018

389. MIT Bitcoin Expo, MIT CSAIL, March 2018

390. ACM-IEEE Lecture, MIT CSAIL, April 2018

391. Media Lab, MIT, April 2018

392. AI Decentralized, Toronto, Canada, May 2018

393. MIT Sloan Fintech Conference, Santiago, Chile, May 2018

394. MIT Fintech Conference, Bueanos Aires, Argentina, May 2018

395. The Future of Fintech, MIT CSAIL, June 2018

396. Blockchain Scientific School, Pula, Italy, June 2018

397. Federated Logic Conference, Oxford, England, July 2018

398. Decentralized Cryptocurrencies and Blockchains, CRYPTO 2018, Santa Barbara, CA, August 2018

399. Keynote, International European Conference on Parallel and Distributed Computing, Barcellona, Spain, August 2018

400. Politecnico di Torino, Torino, Italy, September 2018

401. Politecnico di Milano, Milano, Italy, September 2018

402. Zhejiang Global Lecture, Zhejiang University, China, September 2018

403. Shanghai Iternational Blockchain Week, Shanghai, China, September 2018

404. Hidelberg Laureate Forum, Heidelberg, Germany, September 2018

"Proofs, Knowledge, and Computation"

405. Distinguished Lecture, UC Berkeley, Berkeley, CA, October 2018

"ALGORAND: The Truly Distributed Ledger"

406. Cryptoeconomics and Security Conference, San Francisco, CA, October 2018

407. Lenovo Corporate Strategy Blockchain Summit, Lenovo HQ, Raleigh, NC, October 2018

408. Center for Cryptocurrency Research and Engineering, Imperial College, London, October 2018

409. 5th World Internet Conference, Wuzhen, Zhejang, China, November 2018

Patents

PSEUDO- RANDOM GENERATION

1. U.S. Patent No. 4,944,009: *Pseudo-Random Sequence Generator*

ID SCHEMES

2. U.S. Patent No. 4,879,747: *Method and System for Personal Identification*

3. U.S. Patent No. 4,995,081: *Method and System for Personal Identification Using Proofs of Legitimacy*

4. U.S. Patent No. 5,351,302: *Method for Authenticating Objects Identified by Images or Other Identifying Information*

DIGITAL SIGNATURES

5. U.S. Patent No. 5,016,274: *On-Line/Off-Line Digital Signing*

6. U.S. Patent No. 5,432,852: *Large Provably Fast and Secure Digital Signature Schemes Based on Secure Hash Functions*

7. U.S. Patent No. 5,537,475: *Efficient Digital Signature Algorithm and Use Thereof*

8. U.S. Patent No. 5,638,447: *Compact Digital Signatures*

ENCRYPTION

9. U.S. Patent No. 5,499,296: *Natural Input Encryption and Method of Use*

10. U.S. Patent No. 5,519,778: *Method for Enabling Users of a Cryptosystem to Generate and Use a Private Pair Key for Enciphering Communications Between the Users*

KEY ESCROW

11. U.S. Patent No. 5,276,737: *Fair Cryptosystems and Method of Use*

12. U.S. Patent No. 5,315,658: *Fair Cryptosystems and Method of Use*

13. Canadian Patent No. 2,118,493: *Fair Cryptosystems and Method of Use*

14. Israeli Patent No. 105,471: Fair Cryptosystems and Method of Use

15. EPO Patent No. 0637413: *Verifying Secret Keys in a Public-Key Cryptosystem*

16. Australian Patent No. 670,587: *Verifying Secret Keys in a Public-Key Cryptosystem*

17. Korean Patent No. 151217: *Fair Cryptosystems and Method of Use*

18. British Patent No. 0637413: *Fair Cryptosystems and Methods of Use*

19. British Patent No. 0695485: *Fair Cryptosystems and Methods of Use Thereof*

20. U.S. Patent No. 5,666,414: *Guaranteed Partial Key Escrow*

21. U.S. Patent No. 6,026,163: *Distributed Split-Key Cryptosystem and Applications*

DIGITAL CERTIFICATION AND CERTIFICATE VALIDATION

22. U.S. Patent No. 5,420,927: *Method for Certifying Public Keys in a Digital Signature Scheme*

23. U.S. Patent No. 5,604,804: *Improved Method for Certifying Public Keys in a Digital Signature Scheme*

24. U.S. Patent No. 5,717,759: *Improved Method for Certifying Public Keys in a Digital Signature Scheme*

25. U.S. Patent No. 5,610,982: *Compact Certification with Threshold Signatures*
26. U.S. Patent No. 5,666,416: *Certificate Revocation System*
27. U.S. Patent No. 5,793,868: *Certificate Revocation System*
28. U.S. Patent No. 5,717,758: *Witness-Based Certificate Revocation System*
29. U.S. Patent No. 5,960,083: *Certificate Revocation System*
30. U.S. Patent No. 5,717,757: *Certificate Issue Lists*
31. U.S. Patent No. 6,097,811: *Tree-Based Certificate Revocation System*
32. U.S. Patent No. 6,292,893 B1: *Certificate Revocation System*
33. U.S. Patent No. 6,301,659 B1: *Tree-Based Certificate Revocation System*
34. European Patent No. EP 0 858 702 B1: *Tree-Based Certificate Revocation System*
35. U.S. Patent No. 6,487,658: *Efficient Certificate Revocation*
36. U.S. Patent No. 6,766, 450: Efficient Certificate Revocation

SIMULTANEOUS ELECTRONIC TRANSACTIONS

37. U.S. Patent No. 5,666,420: *Simultaneous Electronic Transactions*
38. U.S. Patent No. 6,134,326: *Simultaneous Electronic Transactions*
39. Canadian Patent No. 2,215,908: *Simultaneous Electronic Transactions*
40. EPO Patent No. *96910516.2: Simultaneous Electronic Transactions;* Nationalized in Italy and the United Kingdom
41. U.S. Patent No. 5,553,145: *Simultaneous Electronic Transactions with Visible Trusted Parties*
42. U.S. Patent No. 5,629,982: *Simultaneous Electronic Transactions with Visible Trusted Parties*
43. U.S. Patent No. 6,137,884: *Simultaneous Electronic Transactions with Visible Trusted Parties*
44. U.S. Patent No. 6,141,750: *Simultaneous Electronic Transactions with Subscriber Verification*

IDEAL ELECTRONIC TRANSACTIONS

45. U.S. Patent No. 5,615,269: *Ideal Electronic Negotiations*

ANONYMOUS TRANSACTIONS

46. U.S. Patent No. 5,790,524: *Anonymous Information Retrieval System*
47. U.S. Patent No. 5,812,670: *Traceable Anonymous Transaction*

Technology Transfer

PATENT LICENSING

1. US Government (Fair Cryptosystems)
2. Bankers Trust (Fair Cryptosystems)
3. Bankers Trust (Simultaneous Electronic Transactions)

COMPANIES

1. ***CoreStreet*** (acquired by ActiveIDentity, 2009)
- Role: *Founder and Inventor of the Core Technologies*
- Core Business: *Real Time Credentials*

2. ***Peppercoin*** (acquired by Chockstone, 2007)
- Role: *Co-Founder and Co-Inventor of the Core Technologies*
- Core Business: *Micropayments*

3. **Algorand** (Founded May 2017)
- Role: Founder and Inventor of the Core Technology
- Business: Distributed Ledgers and Cryptocurrencies